



Near maximum likelihood soft-decision decoding of a particular class of rate-1/2 systematic linear block codes

Patrick Adde, Christophe Jegou, Raphaël Le Bidan

► To cite this version:

Patrick Adde, Christophe Jegou, Raphaël Le Bidan. Near maximum likelihood soft-decision decoding of a particular class of rate-1/2 systematic linear block codes. *Electronics Letters*, 2011, 47 (4), pp.259-260. 10.1049/el.2010.7857 . hal-00573239

HAL Id: hal-00573239

<https://hal.science/hal-00573239>

Submitted on 3 Mar 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Near maximum likelihood soft-decision decoding of a particular class of rate-1/2 systematic linear block codes

P. Adde^{*}, C. Jégo^{**} and R. Le Bidan^{*}

This paper presents a soft-decision decoding algorithm for a particular class of rate-1/2 systematic linear block codes. The proposed algorithm performs successive re-encoding of both the data and parity bits, to produce a list of codewords among which the most likely candidate is chosen. Simulation results show that close to optimal performance can be obtained at reasonable complexity. They validate the potential of the proposed algorithm as a practical approach for soft-decision decoding.

Introduction: This paper focuses on Soft-Decision Decoding (SDD) of a particular class of rate-1/2 ($n=2k, k$) systematic binary linear block codes characterized by the property that their generator matrix \mathbf{G} in canonical form can be written as $\mathbf{G} = [\mathbf{I}_k, \mathbf{P}]$, where \mathbf{I}_k is the $k \times k$ identity matrix and \mathbf{P} is constrained to be a $k \times k$ invertible binary matrix. Note that the considered code family includes self-dual codes as a particular case since the latter satisfy $\mathbf{P}^{-1} = \mathbf{P}^t$ [1]. Many interesting block codes falls into this category, including the (24,12,8) extended Golay code, self-dual Reed-Muller codes, extended quadratic residue codes, or the more recent Cortex codes [2]. The Cortex construction offers a broad spectrum of possibilities for the problem of constructing short linear block codes with good minimum distance properties and low-complexity soft-decision decoders.

Previous work: Maximum-likelihood (ML) soft-decision decoding is known to offer the best decoding performance in terms of block error probability. However it is computationally intractable for most codes of practical interest. Hence sub-optimal SDD algorithms usually have to be considered. Belief Propagation (BP) is a soft-input soft-output decoding algorithm relying on the exchange of soft information along the edges of a graph defined by the parity-check matrix \mathbf{H} of the code [3]. BP is known to closely approximate the performance of optimal Maximum A Posteriori (MAP) decod-

ing at reduced complexity for codes with sparse parity-check matrices. On the other hand, BP performs poorly with most block codes since the latter usually have high-density parity-check matrices, and thus graphs with many short cycles. A very general approach to SDD builds a list of candidate codewords and selects the codeword at minimum Euclidean distance from the received word in this list. Various strategies have been proposed to generate the list. A first category of algorithms performs successive re-encoding of different information sets [4-7]. We recall that an information set is any set of k linearly independent coordinates in an (n,k) linear block code. These k positions uniquely determine the codeword, and thus can be used for systematic encoding. In another family of algorithms, the list is constructed by applying candidate error patterns to the received word and by running a hard-decision decoder on the resulting sequences [8,9]. In both cases, reliability information available at the matched-filter output can be taken into account during the generation of candidate codewords to significantly reduce the list size (and thus the decoding complexity) at a given performance level.

Proposed algorithm: The proposed algorithm falls into the class of reliability-based information-set SDD algorithms. It takes advantage of the code properties to further simplify the decoding process. Assuming Binary Phase-Shift Keying (BPSK) transmission over an Additive White Gaussian Noise (AWGN) channel, the algorithm operates as follows. Let $\mathbf{r} = (r_0, \dots, r_{n-1})$ denote the received sequence at the matched-filter output, and $\mathbf{z} = (z_0, \dots, z_{n-1})$ the corresponding hard-decision sequence ($z_i = 1$ if $r_i > 0$, and 0 otherwise). The vector \mathbf{z} is split into two parts $\mathbf{z} = (\mathbf{z}_s, \mathbf{z}_p)$ by separating the k systematic and k parity coordinates, respectively. A series of N_{ep} error patterns is applied to the k systematic coordinates \mathbf{z}_s which are then re-encoded using the canonical generator matrix $\mathbf{G}_s = [\mathbf{I}_k, \mathbf{P}]$, to produce a first list of N_{ep} candidate codewords. A second list of N_{ep} candidates is obtained by repeating the procedure in parallel on the k parity coordinates \mathbf{z}_p . Re-encoding of the parity set \mathbf{z}_p is realized using the generator matrix $\mathbf{G}_p = \mathbf{P}^{-1} \times \mathbf{G}_s = [\mathbf{P}^{-1}, \mathbf{I}_k]$. By construction, the matrices \mathbf{G}_s and \mathbf{G}_p

are equivalent up to elementary row operations and thus generate the same code. The final decision is given by the candidate codeword at minimum Euclidean distance from the observation \mathbf{r} .

Comparison with other SDD algorithms: Compared to the more general information-set SDD algorithms described in [5][6], the proposed algorithm is computationally much simpler since it does not need to identify the most reliable information set for each received vector, thereby avoiding a costly Gaussian elimination process. Instead, our algorithm takes advantage of the code symmetry to operate on two, fixed information sets, for which encoding functions are easily derived. Further, unlike [8][9], no hard-decision decoder is required. Hence this algorithm can be applied to codes for which no algebraic decoder exists. The error patterns generation strategy also differs from the one used in [5] and [6]. In [5] (see also [10]), error patterns are generated in order of increasing Euclidean weight, whereas order- i ordered-statistics decoding (OSD) in [6] exhaustively tests all combinations of i errors or less in the k most reliable information coordinates. In the proposed algorithm, similarly to the Chase-2 algorithm [9] (see also [7]), the $N_{ep} = 2^p$ candidate error patterns are constructed by testing all configurations of errors confined in the p least reliable positions in each of the considered information set (\mathbf{z}_s or \mathbf{z}_p).

Simulation results: Figure 1 shows the bit-error-rate (BER) performance of the proposed algorithm for the (24,12,8) extended Golay code. For reference purpose, the performance of ML and OSD decoding are also shown. Order-1 and order-2 OSD involve 13 error patterns and 79 error patterns, respectively. We observe that 2×16 error patterns are sufficient to reach near-ML performance with the proposed algorithm. Order-1 OSD performs slightly better with less error patterns, but this comes at a much higher computational cost, due to the Gaussian elimination process. Order-2 OSD achieves ML performance but with 79 error patterns.

The BER performance of several rate-1/2 block codes of length $n=8$ up to 48 under SDD with the proposed algorithm are shown in Figure 2. The considered codes in-

clude classical algebraic constructions such as the (8,4,4) extended Hamming code, the (24,12,8) extended Golay code or the (48,24,12) extended quadratic residue code. The (16,8,5) code was obtained using the Cortex construction. First introduced in [2], Cortex codes are a family of rate-1/2 self-dual systematic linear block codes with good minimum distance properties. The Cortex construction combines a short base code C with a finite sequence of permutations to produce the k parity bits. The reader is referred to [2][11] for a detailed description of the encoding process. The number of error patterns used in the simulations is specified in Table 1. It was optimized in order to obtain performance within 0.05-0.25 dB from ML decoding for each code. For comparison purpose, we also give the number of error patterns required by order- $\lfloor d_{\min}/4 \rfloor$ OSD which was shown in [6] to practically achieve ML for block codes of length $n \leq 128$. These results show that the proposed algorithm is able to achieve near-ML performance at reduced complexity. Indeed, fewer error patterns are necessary and no Gaussian elimination operation (costly in terms of latency and hardware resources) is employed.

Conclusion: A soft-decision decoding algorithm has been introduced for a specific class of rate-1/2 systematic linear block codes which includes in particular the family of self-dual codes. The algorithm performs successive re-encoding of two fixed information sets to produce a list of candidate codewords. Simulation results show that, by taking advantage of the code structure, the proposed algorithm realizes a good trade-off between performance and complexity, thereby providing an attractive alternative to other classical soft-decision decoding algorithms.

References

- [1] R. E. Blahut, *Algebraic codes for data transmission*. Cambridge University Press, 2003.
- [2] J. C. Carlach and C. Vervoux, "A new family of block turbo-codes," in *13th Int. Symp. on Applied Algebra, Algebraic Alg. and Error-Correcting Codes*, Honolulu, USA, November 1999.
- [3] F. R. Kschischang, B. J. Frey, H.-A. Loeliger, "Factor Graphs and the Sum-Product Algorithm," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, Feb. 2001, pp. 498-519.

- [4] J. MacWilliams, "Permutation decoding of systematic codes," *Bell Sys Tech. J.* Jan. 1964, pp. 485--505
- [5] B. G. Dorsch, "A decoding algorithm for binary block codes and J -ary output channels", *IEEE Trans. Inform. Theory*, vol.20, n^o3, pp.391-394, May 1974
- [6] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics", *IEEE Trans. Inform. Theory*, vol.41, n^o5, pp. 1379-1396, Sept.1995
- [7] M. Lalam, K. Amis and D. Leroux, "Sliding window encoding for Reed-Solomon code decoding," in *Proc. 4th Int. Symp. Turbo Codes*, Munich, Germany, April 3-7, 2006
- [8] G. D. Forney Jr, "Generalized minimum distance decoding", *IEEE Trans. Inform. Theory*, vol. 12, n^o2, pp. 125—131, Apr. 1966
- [9] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inform. Theory*, vol IT-18, Jan. 1972, pp 170-182
- [10] A. Valembois & M. P. C. Fossorier, "An improved method to compute lists of binary vectors that optimize a given weight function with application to soft-decision decoding", *IEEE Commun. Lett.*, vol.5, n^o11, pp.456--458, Nov. 2001
- [11] J. E. Perez Chamorro, F. Seguin, C. Lahuec, M. Jezequel, G. Le Mestre, "Decoding a family of dense codes using the sum-product algorithm and subthreshold PMOS," in *Proc. IEEE Int. Symp. Circuits and Systems ISCAS'09*, Taiwan, 24-27 May 2009, Taipei, Taiwan, pp. 2685-2688.

Authors' affiliations:

* Institut TELECOM; TELECOM Bretagne; CNRS Lab-STICC UMR 3192

** CNRS IMS, UMR 5218, 351 Cours de la Libération, 33405 TALENCE, FRANCE

Figure captions:

Figure 1: BER performance of soft decoding of the (24,12,8) Golay code.

Figure 2: Soft-decision decoding performance of different rate-1/2 block codes of length $n=8$ up to 48 with the proposed decoding algorithm

Table

Table 1: Number of error patterns required by the proposed solution and by OSD for different codes $(n, n/2)$ block codes ($n=8$ up to 48).

Figure 1

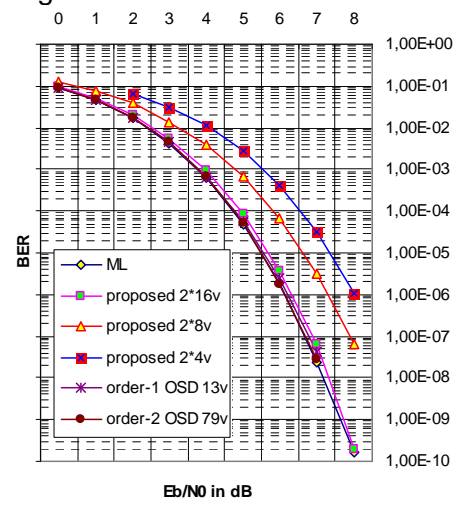


Figure 2

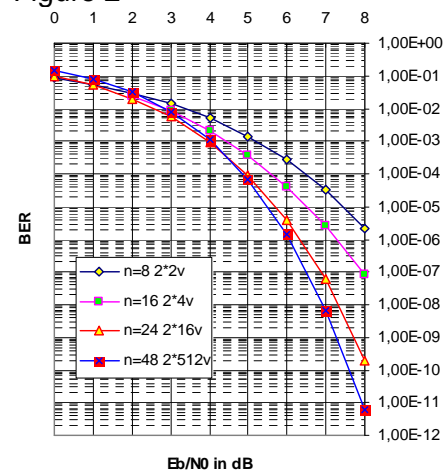


Table 1

| Code | (8,4,4) | (16,8,5) | (24,12,8) | (48,24,12) |
|---|---------|----------|-----------|------------|
| Proposed algorithm | 2×2 | 2×4 | 2×16 | 2×512 |
| Order- $\lfloor d_{\min}/4 \rfloor$ OSD | 5 | 9 | 79 | 2325 |